Chapter 3 Revisions - 2007

030203 Controlling Data Distribution and Transmission

Purpose: To protect the State's data and information from unauthorized disclosure.

STANDARD

Technical access controls or procedures shall be implemented to ensure that data and information are distributed only as authorized and as appropriate. Access controls and/or procedures shall, in part, be based on agency business requirements. Once a business justification is provided, personnel shall adhere to the following standards:

- If information includes both confidential data and data available for public inspection, the classification level shall default to confidential.
- Electronic media entering or leaving offices, processing areas or storage facilities shall be appropriately controlled.
- Storage areas and facilities for media containing confidential data shall be secured and all filing cabinets provided with locking devices.
- Confidential information shall not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements and return dates.
- When confidential information is shipped, the delivery shall be verified.
- All confidential information shall be encrypted when transmitted across wireless or public networks[1], including transmissions such as file transfers and electronic mail.
- Encryption algorithms for the transmission of confidential data include, at a minimum, Secure Socket Layer (SSL) version 3 RC4 128 bit algorithms, SSL Server-Gated Cryptography (SGC) 128 bit algorithms, Transport Layer Security (TLS) version 1.1 128 bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST)[2].

ISO 27002 Reference

9.1 Secure Areas

030205 Managing Electronic Keys

Purpose: To ensure that electronic key systems are managed under proper controls.

STANDARD

[1] Public network includes the State Network.

[2] NIST http://csrc.nist.gov/cryptval/

Agencies using key-based data encryption systems must implement a key-escrow system to guarantee agency access to encrypted data when needed. Key-escrow data shall be routinely backed up. Recovery procedures must be tested at least annually to ensure agency access and availability to encrypted data.

When an agency implements an electronic key system, it must establish proper controls to protect the key and the data encrypted. The system must be designed so that no single person has full knowledge of all keys. The system design must also ensure that:

- Separation of duties or dual control procedures are enforced.
- Any theft or loss of electronic keys results in the notification of management.
- All keys are protected against modification and destruction, and secret/private keys are protected against unauthorized disclosure.
- Physical protection is employed to protect equipment used manage and escrow keys.
- An electronic key management and recovery system, including all relevant key-escrow procedures, is documented and in place.
- Encrypted data are recoverable, at any point in time, even when the person(s) who encrypted the data is no longer available.

Agencies also must comply with the applicable regulations established by the North Carolina Secretary of State.

ISO 27002 References

12.3.1 Policy on the use of cryptographic controls
12.3.5 Key management

030801 Using Encryption Techniques

Purpose: To protect the State's confidential information using encryption techniques.

STANDARD

Each agency shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its method of transmission whether encrypted or unencrypted to a third party not served by the State Network. Encryption techniques shall be employed when encryption is appropriate.

All portable computing devices, including laptops and other mobile computing devices such as personal digital assistants (PDAs) and portable media such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct the public's business, shall use encryption to protect confidential information, including personal information, from unauthorized disclosure.

Agencies using key-based encryption systems must provide for an encryption-key escrow to ensure present and future agency access to encrypted data. Agencies must ensure that only authorized personnel have access to keys used to access confidential information. Proper management control of encryption keys and processes must be ensured when archiving confidential electronic files or documents.

Device	**Encryption Requirements**
Laptop and Notebook	Full Disk (sector-level) - FIPS 140-2 Level 1 certified AES-256 encryption algorithm.
Removable Media such as CDs, memory sticks and, DVDs, or any other portable device that stores data.	Data encrypted using FIPS 140-2 Level 1 certified AES-256 algorithm. Where possible, full disk encryption shall be used. File, volume, or virtual disk encryption may be used to store confidential data when full disk encryption is either not applicable or not possible. Encrypted files containing confidential data shall not be decrypted to removable media. Where possible, government confidential data shall be stored on state issued and owned removable media.
Tape Media	All portable tape media that could contain confidential information, that may be transported or stored off-site, must be encrypted. Agencies should use an encryption algorithm of, at a minimum, 128-bit strength.
Hand-Held Computing Devices, such as smart phones, Blackberry devices, and PDAs,	Confidential data must be encrypted at a minimum using a FIPS 140-2 Level 1 certified AES-128 or Triple-DES encryption[2] algorithm. Where possible, full-disk encryption shall be used. File, volume, or virtual disk encryption may be used to store confidential data when full-disk encryption is either not applicable or not possible.

Agencies shall develop and enforce polices concerning the storage of the State's confidential data on all portable and removable media devices.

GUIDELINES

Agencies should consider encrypting all confidential information or data that would have an adverse impact on the agency's services or functions if their confidentiality were compromised, ~~especially when such information is transmitted to a third party not served by the State Network~~.

Agencies should use an encryption algorithm of, at a minimum, 128-bit strength or one of those accepted and approved by the National Institute of Standards and Technology.

Due to the greater likelihood for theft or loss, users should be instructed to avoid storing confidential information on portable media and devices whenever possible.

For satellite locations, or for locations where weaker physical access controls are present, agencies should strongly consider deploying full-disk encryption on desktops that store confidential information.

RELATED INFORMATION

Standard 010101	Setting Classification Standards—Defining Information
Standard 010102	Setting Classification Standards—Labeling Information
Standard 010103	Setting Classification Standards—Storing and Handling Information
Standard 010104	Setting Classification Standards—Isolating Top Secret Information
Standard 010105	Setting Classification Standards—Classifying Information
Standard 010106	Setting Classification Standards—Custodians of Confidential Information
Standard 010107	Setting Classification Standards—Managing Network Security
Standard 030203	Controlling Data Distribution
Standard 030205	Managing Electronic Keys
Standard 030605	Archiving Electronic Files
Standard 090301	Electronic Eavesdropping

ISO 27002 References

12.3.2	Key management
15.1.6	Regulation of cryptographic controls